

**AVOID BAD ENGINEERING PRACTICES
IN SAFETY INSTRUMENTED SYSTEM DESIGN**

Angela E. Summers, Ph.D., P.E., President, SIS-TECH Solutions, LLC

Published in part: INTECH, November 1999

Introduction

In the decade between 1974 and 1984, three incidents occurred with far reaching consequences to the design, operation, and maintenance of processes in the Chemical Processing Industry (CPI). These incidents were so shocking to the industrial, regulatory, and citizen communities that they simply became known as Flixborough, Seveso, and Bhopal.

Three Incidents That Shaped Process Safety Worldwide:

June 1, 1974 - Flixborough UK: a caprolactam production unit had a release of cyclohexane resulting in an unconfined vapor cloud explosion. The incident caused 56 injuries off-site, as well as 36 injuries and 28 fatalities on-site. On-site, most of the property was severely damaged. The off-site damage was spread over 8 miles, involving over 2400 homes and businesses.

July 10, 1976 – Seveso, Italy: the contents of a 2,4,5-trichlorophenol (TCP) reactor experienced an exothermic, runaway reaction, resulting in the lifting of a rupture disk. A plume containing TCP, caustic, and approximately 1.75 kg dioxin was released, exposing the community to the toxic chemicals. While no permanent injuries or fatalities were reported, approximately 470 people suffered caustic burns, including more than 30 cases of chloracne. More than 4 square kilometers of agricultural land near the site was sterilized for years.

December 2, 1984 – Bhopal, India: a cyanide release occurred due to the introduction of water into a methyl isocyanate storage tank. The release resulted in more than 2500 fatalities and 170,000 injuries. Thousands of the injured were seriously disabled, including long term respiratory and vision damage.

Source: Lees, Frank P., "Loss Prevention in the Process Industries," 2nd edition, Butterworth-Heinemann, Jordon Hill, Oxford (1996).

Due to these incidents, most industrialized nations established process hazards control regulations. Germany passed the Hazardous Incident Ordinance (1980) and the European Community created the Major Accident Hazards Directive (1982). The United States passed legislation creating the Emergency Planning and Community Right-To-Know Act (EPCRA, 1986). In 1990, the Clean Air Act Amendments mandated that the Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA) develop accident prevention regulations, leading eventually to the 1992 OSHA Process Safety Management (PSM) and the 1996 EPA Risk Management Program (RMP) regulations.

None of the regulations were prescriptive. Most were intended to be flexible, simply requiring industry to examine the risk posed by their processes and to work to minimize these risks. Only a few European regulations provided quantitative risk targets. Many European regulations, as well as those of the U.S., relied on industry to develop its own tools to identify risk and to make appropriate efforts to achieve lower risk. As an incentive, industry was required to communicate the identified process risks to the public and emergency responders through public forums and documentation.

The industrial community responded to the regulations by issuing industry standards and guidelines concerning the evaluation of risk and the design of safety systems. The American Petroleum Institute (API), the American Society of Mechanical Engineers (ASME), and the National Fire Protection Agency (NFPA) created codes and practices for specific applications. In 1988, the International Society for Measurement and Control (ISA) began an eight year odyssey to develop a standard for safety instrumented system design (SIS) for the process industries, ANSI/ISA 84.01-1996. In the mid-1980s, the International Electrotechnical Commission (IEC) began the development of an international standard for the design of all safety-related systems, covering transportation, medical, manufacturing, and process industries. This standard, IEC 61508, is expected to be released this year.

In February 1996, ANSI/ISA 84.01-1996, "Application of Safety Instrumented Systems for the Process Industries" (1), was approved by the ISA and, in 1997, it was adopted by the American National Standards Institute (ANSI). This standard is considered by the U.S. Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA) as an *accepted industry practice* (2,3). Any U.S. based instrumented systems specified after March 1997 must be designed in compliance with this standard.

Internationally, IEC 61508, "Functional Safety of Electrical/Electronic/ Programmable Electronic (E/E/PES) Safety-Related Systems," (4,5) is getting very close to being released as a final standard. The standard consists of seven parts, four of which have already been issued as final and three are waiting for final vote on the final draft international standard (FDIS). The intent is to release the entire standard as final before the end of 1999. Instrumented systems designed in the next millennium will be required to comply with this standard, with the exception of U.S. installations that must follow ANSI/ISA 84.01-1996.

Consequently, it is regulations the mandate that industry identify and address risk. Industry standards are simply providing the tools for assessing the adequacy of industry's efforts. The difficult task of creating one standard for all of the process industry made the creation of a prescriptive standard impossible. After all, could one prescriptive standard cover refinery furnaces, chemical reactors, pulp and paper digesters, and utility boilers and reduce risk appropriately at a reasonable cost? Thus, the standards had to be performance based. Both standards chose to rely on the establishment of a design process called the SIS lifecycle, throughout which the performance of the instrumented systems must be maintained.

The lifecycle is intended to address the primary causes of control system incidents. In the book, Out of Control (6), the HSE examined 34 incidents that were due to control system failures. Their analysis was based on five defined phases: specification, design and implementation, installation and commissioning, operation and maintenance, and changes after commissioning. The results, as shown in Figure 1, clearly indicate that all phases must be addressed in order to minimize the potential for incident. For this reason, the industry standards approach SIS design based on the lifecycle process, covering all phases of design from conception to decommissioning.

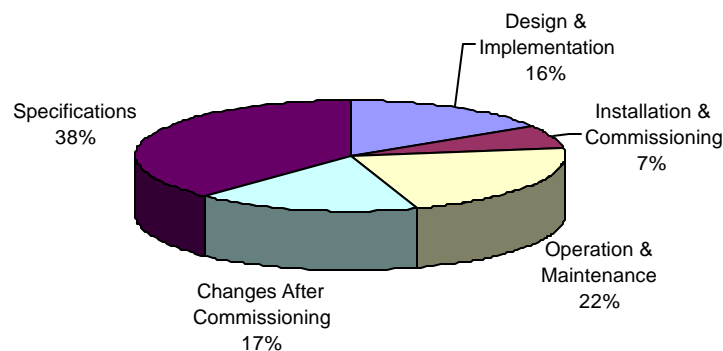


Figure 1: HSE Concerning the Root Causes of Control System Incidents

Compliance with the industrial standards, ANSI/ISA 84.01-1996 and IEC 61508, requires four essential elements:

1. identification of safety functions required for safe shutdown;
2. assignment of a safety integrity level (SIL) for each safety function;
3. use of the safety lifecycle for the SIS design; and
4. verification of the SIL achieved for each safety function.

These elements result in a major paradigm shift for SIS design. While it has been accepted practice for many years to mitigate potential incidents with instrumented systems, there has generally been no assessment of what type of SIS provides the appropriate risk reduction. These standards have now established requirements that industry document the rationale behind the use of a particular design, evaluate that design for its integrity, and demonstrate that the integrity can be maintained. This is perhaps the most significant impact of ANSI/ISA 84.01-1996 and IEC 61508 on process safety, in general.

As performance based standards, the race for compliance is marked with the broadly defined finish line of good engineering practice and highly recommended practices. As industry races toward compliance, it must work hard to prevent the creation and acceptance of bad engineering practices, which threaten the economics of plant operation and erode the effectiveness of SIS designs. This paper will address seven bad engineering practices:

Seven Bad Engineering Practices in SIS Design:

1. Believing that, if something is not specifically stated, either “shall do” or “shall not do,” in the standards, you do not have to worry about it
2. Thinking that meeting the minimum requirements means the process is safe and the SIS is compliant with the standard
3. Ignoring the importance of good engineering practice
4. Designing systems that meet safety requirements but not economic protection requirements
5. Focusing only on SIL and not on preventing nuisance trips
6. Neglecting the human factors
7. Focusing on capital cost and not lifecycle costs

1. Believing that, if something is not specifically stated, either “shall do” or “shall not do,” in the standards, you do not have to worry about it.

Some engineers think that compliance with the standards is “much ado about nothing,” since there are only a few specific requirements. Even when specific requirements do exist, there is typically a statement that the User could choose to do otherwise, if a process hazards analysis shows that an alternative does not reduce the safety integrity. This has led some engineers to argue that they do not have to follow some recommended practices, since they are not specifically required by the standard.

While the standards lack many specific requirements, the standards do establish a process that ensures that the SIS design is carefully chosen and that the selection criteria are thoroughly documented. This documentation becomes part of the process safety information that must be maintained along with any documented justification for changes to the SIS. This documentation contains the rationale for the SIS design. As a result, the lawyers on both sides of any liability suit or regulatory action will request this documentation for comparison with engineering practice and standards adherence.

Therefore, while the standards rely on performance criteria for determining the appropriateness of the SIS design, this flexibility does not mean that the standard is without significance or that the requirements can be ignored. Flexibility allows the User to mold the lifecycle approach for their specific application. This ensures that the resources spent on the SIS are appropriate for the risk and that the final system design fits the operational philosophy of the facility. Moreover, due to the lack of specific requirements, the standard provides an open door for the adoption of new technologies. The performance criterion provides a constraint on the use of new technologies, since they must be proven to be effective in the mitigation of process risk. Thus, it allows the examination of design alternatives, as long as these alternatives provide as safe or safer installations.

The User is ultimately responsible for safe operation of the process. The standards were written with this principle in mind. Flexibility of design choice does not reduce this responsibility.

2. Thinking that meeting the minimum requirements means the process is safe and the SIS is compliant with the standard.

The standards require that the User evaluate the non-SIS layers of protection or the external risk reduction facilities. If the risk reduction from these layers does not reduce the risk to a tolerable level, a SIS can be used to further reduce the risk. The required SIS functionality and target SIL is determined and documented during this assessment. No minimum requirements are included for these essential decisions. However, without question, if the SIS functionality and target SIL are incorrectly chosen, the SIS will not reduce the risk as intended. In fact, the SIS may make the situation worse.

Meeting the minimum requirements will not protect the engineer or the facility from liability associated with incidents. Issuing a report, which states that the risk is negligible so no SIS is required, may fulfill the documentation requirements, but it definitely does not fulfill the intent of the standard if the risk would not be considered negligible by industry. The nature of good engineering practice and due diligence means that whatever is done for a specific application must be similar to what has been done in similar applications at other facilities within the process industry.

3. Ignoring the importance of good engineering practice.

As engineers begin to work toward standards compliance, there is a tendency among the best, most talented engineers to want to make sure that there is no question with regard to their design. This means that many engineers will want every decision with respect to the SIS design proven for agreement with the SIL or some specific clause in the standards. Corporate design guidelines and engineering practices have evolved over the years in the direction of providing more safety available and reliable SISs. Once these practices have been validated, there is no need to continually re-validate them.

The quantitative assessment only includes the instruments required for the SIS functionality. There are many other design decisions that must be made that affect the SIS long-term operational integrity. No numerical tool or design standard can replace experienced, knowledgeable engineers. The installed performance of instrumentation, including operating

environment, process impact and wiring practices, cannot be covered in detail for every application in any industry standard.

Occasionally, a User will find out that what they have deemed normal practice does not provide adequate protection. This is part of the normal learning process whenever a new standard or regulation changes how an engineer views a system. This complexity makes design experience more important, because changes to design practice must be thought through carefully to ensure that the final design is actually the most appropriate.

4. Designing systems that meet safety requirements but not economic protection requirements.

While the SIS standards are focused on safety impacts, the lifecycle process can be used in any situation where the incident risk is unacceptable and an instrumented system is selected to mitigate this risk. There are many applications where the economic justification for the use of an instrumented system is substantially higher than the safety justification. The safety emphasis of the standards should not lead engineers to ignore the importance of effective design for economic protection systems.

For example, a manager with a large refinery reported that a hazards assessment of some furnaces had yielded very few safety concerns. Therefore, he felt that he did not have to be concerned with the SIS standards. On further discussion, it was determined that an incident in these furnaces would result in significant equipment damage and downtime. The economic impact from many of the incident scenarios was severe.

Fortunately, the lifecycle approach is sufficiently broad to allow the standards to be applied to economic protection systems, as well as safety-related systems. The main change to the SIS lifecycle is that an economic integrity level (EIL) is chosen in addition to any SIL requirement. The final design would be based on the highest required integrity level whether safety or economic related. The remainder of the lifecycle can then be used with little modification.

5. Focusing only on SIL and not on preventing nuisance trips.

The most important SIS performance criterion is the safety integrity level (SIL). The SIL is chosen by the User based on their knowledge of the potential frequency of undesired incidents and the consequences of these incidents. As discussed previously, the underlying principle of the standards is that the User has the responsibility to choose the appropriate SIL and to determine how to design, operate, maintain, and test the SIS to maintain the SIL.

In viewing the safe operation of a facility, it is important to look at nuisance trip rate also.

Consider the following example:

A small chemical company had a series of tanks with overpressure protection trips. The shutdown system on each tank consisted of pressure switches, relays, and valves with associated solenoids. Four pressure switches were installed 1oo4. From a safety point of view, this is an extremely safe architecture, since it only requires that one of the pressure switches work properly for the safe shutdown to occur.

Unfortunately, the unit experienced several nuisance trips each year due to faulty pressure switch action. The operators became very accustomed to the occurrence of the shutdown and routinely assumed that it was caused by the pressure switches. They did not troubleshoot or investigate the cause of overpressure trips. They simply restarted the unit. For further rationalization, they convinced themselves that if the pressure was indeed a real problem that the unit would trip again. Unfortunately, on one occasion the trip was real, the restart action resulted in high pressure and the pressure switches functioned, but the valve did not close. The head of one of the tanks was blown off and landed a hundred feet away narrowly missing a large chemical storage tank.

In this example, the nuisance trips had led the operators to ignore the shutdown, which eventually led to a hazardous incident. While this example may seem extreme, it is not uncommon to walk into a control room and see alarms being ignored or acknowledged without investigation, because the operators do not trust the instrumentation. Nuisance trips can impact the safety of a facility by causing the operators to ignore alarms. Furthermore, most nuisance trips result in the activation of other safety systems, such as cascade trips in other units or the lifting of pressure

relief valves. Finally, industry data has shown that incidents are much more likely during start-up than during normal operation. A nuisance trip leads to start-up. Consequently, nuisance trips are not always just an irritation.

The standards do not emphasize nuisance trips, because the standards are focused on safety. Nuisance trips are viewed as an on-line, an up-time, or a reliability issue. When the plant is down, it is not making product; it is not making money. However, nuisance trips are important from a safety perspective, as well as from an economic perspective.

6. Neglecting the human factors.

The standards acknowledge that humans are important to successful SIS operation. Correct actions are required from all of the personnel associated with the design, installation, commissioning, operation, maintenance, testing, and modification of the SIS. Any poor decision, mistake, or error made at any stage of design could prevent the proper operation of the SIS. For example, if a maintenance person incorrectly calibrates the trip transmitter, it really does not matter what everyone else did to make sure that the SIS for that safety function was validated for its SIL.

Administrative procedures must be developed that ensure that the potential for humans to impact SIS operation is minimized. Examples of administrative procedures would include, but are not limited to, the following:

- Detailed testing/maintenance procedures written from the maintenance personnel perspective, including check-off and initial blanks
- Access restrictions to SIS components, including levels of approval based on requested access
- Authorization requirements for bypassing of any SIS safety function, including time allotted for bypassing without additional approval
- Specific management of change (MOC) requirements for the SIS
- Independent auditing of compliance with any procedure relating to safe operation

These administrative procedures can seriously reduce the potential impact to the successful operation of any installed SIS.

In addition to administrative procedures, SIS designers have a responsibility to create designs that minimize the potential for human impact to the design integrity. Last year, an engineer developed a SIL 3 design for the overpressure protection of a large gas pipeline. The engineer had been instructed that the SIS should be designed to minimize the potential for common cause failure. The proposed design consisted of three transmitters, a redundant PLC, and two trip valves with solenoids. Due to the concern for common mode failure, the three transmitters were specified as coming from three different Vendors. The engineer felt that this would reduce the common mode failure due to potential manufacturing and design flaws.

On paper, this design looks good. A quantitative assessment, provided by many risk analysts, would agree that this is a good design. However, the choice is wrong, because everyone forgot about the maintenance department. The probability that the maintenance technician will incorrectly test and repair the transmitter is higher due to the fact that the technician has to have three different sets of equipment and three different procedures. Any risk assessment of this design must include this as a factor. When transmitters are selected from a single Vendor, the probability that the maintenance technician incorrectly testing and repairing the transmitter is significantly reduced. The impact of design and manufacturing faults can also be reduced by using components from reputable Vendors, with proven performance in the specific application, and by thoroughly testing the component prior to start-up.

7. Focusing on capital cost and not lifecycle costs.

In early times, necessity was the mother of invention. In the economic reality of today's engineer, cost management drives innovation. The greatest concern for a project manager is installed cost, which typically includes design and capital costs. However, in order to achieve the most cost effective design, the lifecycle cost must also be considered. To illustrate, look at the following examples of costs that should be included:

- Testing costs: The minimum design cost would be the installation of one switch, a relay, and a single solenoid/valve. In a SIL 3 application, this architecture would require frequent testing, which can substantially increase maintenance costs for the facility. With reductions in the maintenance staff, this testing frequency may not be maintained, resulting in a lower safety integrity than required.

- Nuisance trip costs: A nuisance trip in an ethylene plant costs more than US\$500,000, resulting from lost production and downtime. If a minimum installed cost architecture is selected which has a high nuisance trip rate, one nuisance trip is sufficient to eliminate any savings in initial capital costs.
- Commissioning and modification costs: Relays can provide the lowest installed cost on a per loop basis when only design and installation is considered. However, commissioning costs are typically much higher in relay applications than in programmable logic controller (PLC) applications. Moreover, the modification costs are substantially higher when those modifications involve relays rather than PLCs. For example, if the SIS uses 1002 sensors for the process input and a third sensor is going to be installed, the modification cost associated with adding the logic to the PLC is smaller than field modification of the relay system.

All costs associated with the SIS lifecycle should be considered when making the SIS decisions. The standards have changed how engineers approach SIS design. Smart engineers will also change how they view the SIS cost.

Summary

The regulatory community is requiring that industry acknowledge and minimize the risk that they pose to the citizen community. Industry's first step for SIS design was the development of ANSI/ISA 84.01-1996 and draft IEC 61508. The linking of process risk and required SIS performance is a concept that was a long-time coming, but, without a doubt, it is a concept that will make the CPI safer.

The judgment on whether industry is safe enough will be made by the community. They will tally the incidents, in terms of frequency and consequence. They will watch the television news and read the newspapers, concerning fires, explosions and chemical releases. They will pay close attention to industry's injury and fatality statistics. If they judge that industry is not safe enough, regulations will be written and this process will begin again.

The judgment of whether industry is successful will be made by the marketplace. At the end of a quarter or a year, success or failure is a matter of dollars and cents. In a global economy, competition can only be fair if the playing field is level. With regard to the use of safety instrumented systems, the standards level the playing field. They provide minimum performance

guidelines. They require that all industry rise to the level of the good corporate citizen, who has been working toward risk reduction for many years.

Finally, the standards provide ways to justify the costs of instrumented systems by analyzing the risk reduction benefits of SIS implementation. When engineers utilize the lifecycle process, engineers will find that, when the standards are correctly used, it is possible to be both successful in the marketplace and safe for the community.

References

1. Hazardous Incident Ordinance, St`rfallverordnung, 1980.
2. Major Accident Hazards Directive, 82/501/EEC, 1982.
3. "Emergency Planning and Community Right-To-Know Act," Environmental Protection Agency, 1996.
4. "Risk Management Programs for Chemical Accidental Release Prevention," 40 CFR Part 68, EPA, Washington (1996).
5. "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," 29 CFR Part 1910, OSHA, Washington (1992).
6. "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA-ISA 84.01-1996, ISA, Research Triangle Park, NC (1996).
7. "Functional safety of electrical/electronic/programmable electronic safety related systems," Parts 1, 3, 4, and 5, IEC 61508, 65A/255/CDV, International Electrotechnical Commission, Final Standard, December 1998.
8. "Functional safety of electrical/electronic/programmable electronic safety related systems," Parts 2, 6, and 7, IEC 61508, 65A/255/CDV, International Electrotechnical Commission, Final Draft International Standard, January 1999.
9. "Control systems: Why things went wrong, and how they could have been prevented," Health & Safety Executive Books, Sudbury, Suffolk, United Kingdom.